UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,012	01/21/2004	Reid Kuhn	MS1-1763US	4493

22801   7590   02/19/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
LE, CANH

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
02/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/762,012	KUHN ET AL.
	Examiner	Art Unit	
	Canh Le	2139	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _11/27/2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _1-3, 7-22, 24-32, 36-51, 53-59 and 61-68_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-3, 7-22, 24-32, 36-51, 53-59 and 61-68_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the amendment filed on 11/27/2007.

Claims 4-6, 23, 33-35, 52 and 60 have been cancelled.

Claims 1, 3, 7-9, 11, 19, 24-26, 30, 32, 36, 38, 40, 48, 53-55, 59, 61, 62, 65, 66 and 68 have been amended.

Claims 1-3, 7-22, 24-32, 36-51, 53-59, and 61-68 have been examined and are pending.

Response to Arguments

Applicant's arguments filed 11/27/2007 have been fully considered but they are not persuasive.

With regard to claim 1, on pages 27-30, the Applicant argues that "Chung does not anticipate this claim because it does not show or disclose the following elements as recited in this claim:

- "with second logic that is operatively coupled to said first logic, modifying said authentication request by including certificate information in a modified authentication request"

- "with said authentication logic, outputting an authentication response comprising authentication approval information and corresponding cryptography information"".

The Examiner respectfully disagrees

Chung teaches a registration comprises a computer and server in communication

via a network, an internet and/or the Internet, means for entry of data into the computer,

and a signature or biometric digitizer including coupling software for directly entering

digitized signature or biometric data electronically into the computer. Chung is silent

about the authentication request including certificate information and authentication

response comprising authentication approval information and corresponding

cryptography information. However, Howard teaches about including certificate

information in a modified authentication request [par. [0018], lines 5-8] and Stanko

teaches with said authenticating logic, outputting an authentication response comprising

authentication approval information and corresponding cryptography information [par.

[0047]; lines 6-13; par. [0048], lines 9-11] (See more details Office action below).

With regard to claim 1, on pages 31-33, the Applicant argues about "the combination of

Chung, Stanko, and Howard does not teach all of the elements as specified in claim 1.

The references, alone or in combination, do not disclose the step of modifying, using

certificate information, an authentication request that has already been cryptographically

modified".

The Examiner respectfully disagrees

In response to applicant's argument that there is no suggestion to combine the

references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). Stanko teaches the limitations which Chung does not teach such as an authentication response comprising authentication approval information and corresponding cryptography information [par. [0047]; lines 6-13; par. [0048], lines 9-11] and Howard teaches limitation which Chung does not teach such as certificate information in a modified authentication request [par. [0018]]. The combination of Chung, Stanko, and Howard teach the subject matter in the independent claim 1. Therefore, the combination of teaching Chung, Stanko, and Howard is proper (See more details Office action below).

With respect to the Applicant's argument against claims 30, 59, 66, and 68, The Applicant merely states that the claimed elements of those claims are being argued in a similar fashion as to claim 1. However, the Examiner has responded to the arguments against claim 1 above. Furthermore, the rejections to claims 30, 59, 66, and 68 would also stand similar to claim 1. Since independent claims 1, 30, 59, and 66 stand rejected, the claims depended therefrom, which are not argued by the applicant, are also rejected.

The fact that Examiner may not have specifically responded to any particular arguments made by Applicant and Applicant's Representative should not be construed as indicating Examiner's agreement therewith.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 7-14, 19-22, 24, 25-26, 27, 30-32, 36-43, 48-51, 53, 54-55, 56, 59, 61-63, 65-67, and 68 are rejected under 35 U.S.C. 103(a) as being anticipated by **Chung et al.** (US 2003/0026462 A1) in view of **Stanko** (US Patent 20050074126 A1) and further in view of **Howard** et al. (US 2004/0103064 A1).

As per claim 1:

Chung teaches a method comprising:

(a) establishing authentication information, said authentication information including time information associated with authenticating logic **[par. [0079]; lines 5-12; "Signature or other biometric data should be captured substantially in "real time" with a reliable date/time stamp made part of the signature or other biometric data**

record along with the digitized signature or other biometric"; an authentication

information includes signature or biometric plus time stamp];

(b) with first logic, establishing credential information **[par. [0079]; "Signature**

or other biometric data should be captured substantially in "real time" with a

reliable date/time stamp made part of the signature or other biometric data

record along with the digitized signature or other biometric"; establishing

credential information is equivalent to "signature or other biometric data should

be captured"]; and

(c) outputting an authentication request comprising said authentication

information and said credential information, said authentication request being

cryptographically modified **[par. [0083], "The digitized signature or other biometric**

and/or other data should be encrypted when transmitted over the Internet, e.g.,

utilizing 128-bit or greater encryption coding". An authentication information

includes signature or biometric plus time stamp should be encrypted when

transmitted over the internet].

(d) with second logic that is operatively coupled to said first logic, modifying

said authentication request **[par. [0083], "The digitized signature or other biometric**

and/or other data should be encrypted when transmitted over the Internet, e.g.,

utilizing 128-bit or greater encryption coding"; The logic has capable to select a

signature or other biometric to output a modified authentication request].

(e) with authenticating logic that is operatively configured to receive said

modified authentication request, at least validating said authentication

information, and authenticating said credential information **[fig. 9; par. [0117]; "Upon**

or after receipt, voter registration file 410 is read 420 and the encoded registration

information 412 and digitized signature data 414 are separated 425 from the

relational encryption code 416, and, if encrypted, are decrypted. The validity of

the encoded data 412, 414 is then compared 430 to determine whether the data

412 and/or 414 is/are valid relative to encryption code 416"]; and

Chung is silent with said authenticating logic, outputting an authentication

response comprising authentication approval information and corresponding

cryptography information.

However, Stanko teaches,

(f) with said authenticating logic, outputting an authentication response

comprising authentication approval information and corresponding cryptography

information **[par. [0047]; lines 6-13; "Authentication server 208 can use any**

credentials that can be transmitted across HTTP to authenticate client 202,

including passwords, challenge-response, digital certificates, tokens, smart

cards, or biometrics, or any combination thereof, and can authenticate against

any backend directory via lightweight directory access protocol (LDAP),

Microsoft Windows NT LAN Manager (NTLM), or another protocol"; par. [0048],

lines 9-11; An authentication approval information is equivalent to a token (or

ticket)].

Therefore, it would have been obvious to the person of ordinary skill in the art at

the time the invention was made to modify method of Chung of the invention by

including the step of Stanko because it would enable client 202 to access secure server

204A automatically **[Stanko, par. [0049], lines 1-2].**

Chung is silent about including certificate information in a modified authentication

request.

However, Howard teaches about including certificate information in a modified

authentication request **[par. [0018], lines 5-8; "User PC 10 then contacts**

authentication server 30 through Internet 20 A serial number 48 and an encrypted

certificate 49 are sent to authentication server 30"].

Therefore, it would have been obvious to the person of ordinary skill in the art at

the time the invention was made to combine method of Chung and a security credential

message includes at least one security credential (e.g. password, challenge-response,

digital certificates, tokens, smart card, or biometrics,..) belonging to the user of client

202 **[Stanko; par. [0047]]** of Stanko of the invention by including the step of Howard

because it would help to reduce fraud through password sharing associated with the

prior art method of access **[Howard, par. [0013], lines 12-15].**

As per claim 2:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, wherein said first logic is

configured to output said authentication request **[par. [0083], "The digitized**

signature or other biometric and/or other data should be encrypted when

transmitted over the Internet, e.g., utilizing 128-bit or greater encryption

coding"].

As per claim 3:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, wherein said second logic

is configured to output said modified authentication request **[par. [0083], "The digitized**

signature or other biometric and/or other data should be encrypted when

transmitted over the Internet, e.g., utilizing 128-bit or greater encryption coding";

A logic includes a first logic and a second logic].

As per claim 7:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Stanko further teaches the method as recited in claim 1, further comprising:

with said first logic, accessing at least a portion of said authentication response to

retrieve said corresponding cryptography information and outputting said retrieved

cryptography information **[par. [0047]; lines 6-13; "Authentication server 208 can**

use any credentials that can be transmitted across HTTP to authenticate client

202, including passwords, challenge-response, digital certificates, tokens, smart

cards, or biometrics, or any combination thereof, and can authenticate against

any backend directory via lightweight directory access protocol (LDAP),

Microsoft Windows NT LAN Manager (NTLM), or another protocol"; par. [0048],

lines 9-11; An authentication approval information is equivalent to a token (or

ticket); A client (i.e. first logic and second logic) has capable to access at least a

portion of authentication response (i.e. token)].

As per claim 8:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Stanko further teaches the method as recited in claim 7, further comprising:

with said second logic that is operatively coupled to said first logic and said

authentication logic, accessing at least a portion of said authentication response and

using said retrieved cryptography information retrieve said authentication approval

information **[par. [0047]; lines 6-13; "Authentication server 208 can use any**

credentials that can be transmitted across HTTP to authenticate client 202,

including passwords, challenge-response, digital certificates, tokens, smart

cards, or biometrics, or any combination thereof, and can authenticate against

any backend directory via lightweight directory access protocol (LDAP),

Microsoft Windows NT LAN Manager (NTLM), or another protocol"; par. [0048],

lines 9-11; An authentication approval information is equivalent to a token (or

ticket); A client (i.e. first logic and second logic) has capable to access at least a

portion of authentication response (i.e. token or ticket); par. [0049], lines 8-10;

"Authentication server 208 also applies a digital signature to the ticket using a

public-private key pair"; retrieving cryptograph information can be digital

signature].

As per claim 9:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, further comprising:

with said second logic, accessing at least a portion of said authentication

response to retrieve said corresponding cryptography information **[par. [0047]; lines 6-**

13; "Authentication server 208 can use any credentials that can be transmitted

across HTTP to authenticate client 202, including passwords, challenge-

response, digital certificates, tokens, smart cards, or biometrics, or any

combination thereof, and can authenticate against any backend directory via

lightweight directory access protocol (LDAP), Microsoft Windows NT LAN

Manager (NTLM), or another protocol". Par. [0048]; lines 9-11; An authentication

approval information is equivalent to a token (or ticket); A client (i.e. first logic

and second logic) has capable to access at least a portion of authentication

response (i.e. token)].

As per claim 10:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung teaches the method as recited in claim 9, further comprising:

with said second logic, accessing at least a portion of said authentication

response and using said retrieved cryptography information retrieve said authentication

approval information **[par. [0047]; lines 6-13; "Authentication server 208 can use**

any credentials that can be transmitted across HTTP to authenticate client 202,

including passwords, challenge-response, digital certificates, tokens, smart

cards, or biometrics, or any combination thereof, and can authenticate against

any backend directory via lightweight directory access protocol (LDAP),

Microsoft Windows NT LAN Manager (NTLM), or another protocol". Par. [0048];

Lines 9-11; An authentication approval information is equivalent to a token (or

ticket); A client (i.e. first logic and second logic) has capable to access at least a

portion of authentication response (i.e. token or ticket); par. [0049], lines 8-10;

"Authentication server 208 also applies a digital signature to the ticket using a

public-private key pair"; retrieving cryptograph information can be digital

signature].

As per claim 11:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, wherein said

authentication request is cryptographically modified by encryption using a private key

[par. [0128]; lines 5-11; "security for data and information transmitted via

networks, the Internet and other communication media may be provided by any

one or more of a relational check code or number, public or private key

encryption, a 128-bit encryption protocol, or any other encryption and/or data

protection scheme, whether more or less secure, whether available presently or

in the future"; par. [0083], "The digitized signature or other biometric and/or other

data should be encrypted when transmitted over the Internet, e.g., utilizing 128-bit

or greater encryption coding". An authentication information includes signature

or biometric plus time stamp should be encrypted by private key when

transmitted over the internet].

As per claims 12, 13:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

A private key is associated with a logic, which includes a first logic and second

logic. Claims 12 and 13 are rejected with the same reason as in claim 11.

As per claim 14:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Stanko further teaches the method as recited in claim 11, further comprising:

with said authenticating logic, retrieving said authentication information and said credential information from said authentication request using a public key pair-wise associated with said private key **[par. [0049]; lines 8-10; par. [0051], lines 5-9; "secure server 204A retrieves the public key corresponding to the private key used to apply the digital signature to the ticket, uses it to verify the digital signature, and grants access to client 202 (that is, establishes the session)"].**

As per claim 19:

The combination of teaching Chung, Stanko, and Howard teach the claimed subject matter.

Chung further teaches the method as recited in claim 8, wherein said first logic is provided at least in a first device that includes a credential gathering mechanism configurable to establish said credential information, said second logic is provided in at least a second device, and said authenticating logic is provided in at least a third device **[par. [0079]; lines 5-12; "Signature or other biometric data should be captured substantially in "real time" with a reliable date/time stamp made part of the signature or other biometric data record along with the digitized signature or other biometric"; establishing credential information is equivalent to "signature or other biometric data should be captured"; A logic includes a first logic and a second logic; par. [0083]; "The digitized signature or other biometric and/or other data should be encrypted when transmitted over the Internet, e.g., utilizing 128-bit**

or greater encryption coding". An authentication information includes signature or biometric plus time stamp should be encrypted when transmitted over the internet].

As per claim 20:

The combination of teaching Chung, Stanko, and Howard teach the claimed subject matter.

Chung further teaches the method as recited in claim 19, wherein said credential gathering mechanism is configurable to establish biometric information **[par. [0079]; lines 5-12; "Signature or other biometric data should be captured substantially in "real time" with a reliable date/time stamp made part of the signature or other biometric data record along with the digitized signature or other biometric"].**

As per claim 21:

The combination of teaching Chung, Stanko, and Howard teach the claimed subject matter.

Chung further teaches the method as recited in claim 19, wherein said second device includes at least one computer operatively configured as a client device, and said third device includes a computer operatively configured as a server device **[abstract; par. [007]; "computer and a server in communication via a network, an intranet and/or the Internet, means for entry of data into the computer, and a signature or biometric digitizer including coupling software for directly entering**

digitized signature or biometric data electronically into the computer. The data

and digitized signature or biometric data may be communicated to the server";

fig. 3].

As per claim 22:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 19, further comprising:

generating said authentication information using at least one logic selected from

said second logic and said authenticating logic [par. [0083]; "The digitized signature

or other biometric and/or other data should be encrypted when transmitted over

the Internet, e.g., utilizing 128-bit or greater encryption coding"].

As per claim 24:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Howard further teaches that an authenticating logic is configured to validate said

authentication request based at least in part on said certificate information [par. [0020],

lines 6-8; "When authentication server 30 receives serial number 48 and

encrypted certificate 49, it can apply master key 53 to verify the identity of smart

card 14"].

As per claim 25:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, wherein said

authenticating logic is configured to validate said authentication information based on at

least nonce data and timestamp data within said authentication information **[par.**

[0079]; lines 5-12; "Signature or other biometric data should be captured

substantially in "real time" with a reliable date/time stamp made part of the

signature or other biometric data record along with the digitized signature or

other biometric"; an authentication information includes signature or biometric

plus time stamp; fig. 9; par. [0117]; "Upon or after receipt, voter registration file

410 is read 420 and the encoded registration information 412 and digitized

signature data 414 are separated 425 from the relational encryption code 416,

and, if encrypted, are decrypted. The validity of the encoded data 412, 414 is then

compared 430 to determine whether the data 412 and/or 414 is/are valid relative to

encryption code 416"].

As per claim 26:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Chung further teaches the method as recited in claim 1, wherein said

authenticating logic is configured to authenticate said credential information by logically

comparing said credential information with stored credential information **[par. [0079];**

lines 5-12; "Signature or other biometric data should be captured substantially in

"real time" with a reliable date/time stamp made part of the signature or other

biometric data record along with the digitized signature or other biometric"; an

authentication information includes signature or biometric plus time stamp; fig. 9;

par. [0117]; "Upon or after receipt, voter registration file 410 is read 420 and the

encoded registration information 412 and digitized signature data 414 are

separated 425 from the relational encryption code 416, and, if encrypted, are

decrypted. The validity of the encoded data 412, 414 is then compared 430 to

determine whether the data 412 and/or 414 is/are valid relative to encryption code

416"; fig. 1; par. [0028]; lines 1-11; county level database 20 and central database

30].

As per claim 27:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Stanko further teaches the method as recited in claim 8, wherein said

authentication approval information includes an access token for use by said second

device **[par. [0047]; lines 6-13; "Authentication server 208 can use any credentials**

that can be transmitted across HTTP to authenticate client 202, including

passwords, challenge-response, digital certificates, tokens, smart cards, or

biometrics, or any combination thereof, and can authenticate against any

backend directory via lightweight directory access protocol (LDAP), Microsoft

Windows NT LAN Manager (NTLM), or another protocol"; par. [0048], lines 9-11;

An authentication approval information is equivalent to a token (or ticket)].

Claim 30 is essentially the same as claim 1 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 31 is essentially the same as claim 2 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 32 is essentially the same as claims 1 and 3 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 36 is essentially the same as claim 7 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 37 is essentially the same as claim 8 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 38 is essentially the same as claim 9 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 39 is essentially the same as claim 10 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 40 is essentially the same as claim 11 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 41 is essentially the same as claim 12 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 42 is essentially the same as claim 13 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 43 is essentially the same as claim 14 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 48 is essentially the same as claim 19 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 49 is essentially the same as claim 20 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 50 is essentially the same as claim 21 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 51 is essentially the same as claim 22 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 53 is essentially the same as claim 24 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 54 is essentially the same as claim 25 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 55 is essentially the same as claim 26 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 56 is essentially the same as claim 27 except that it sets forth the claimed invention as computer readable medium rather a method and rejected under the same reasons as applied above.

Claim 59 is essentially the same as claims 1-3 except that it sets forth the claimed invention as system rather a method and rejected under the same reasons as applied above.

Claim 61 is essentially the same as claim 27 except that it sets forth the claimed

invention as a system rather a method and rejected under the same reasons as applied

above.

Claim 62 is essentially the same as claims 7-8 except that it sets forth the claimed

invention as a system rather a method and rejected under the same reasons as applied

above.

Claim 63 is essentially the same as claims 12 and 14 except that it sets forth the

claimed invention as a system rather a method and rejected under the same reasons as

applied above.

Claim 65 is essentially the same as claims 7-8 except that it sets forth the claimed

invention as a system rather a method and rejected under the same reasons as applied

above.

Claim 66 is essentially the same as claim 1 except that it sets forth the claimed

invention as an apparatus rather a method and rejected under the same reasons as

applied above.

Claim 67 is essentially the same as claims 1, 7-8, and 19-20 except that it sets forth the

claimed invention as an apparatus rather a method and rejected under the same

reasons as applied above.

Claim 68 is essentially the same as claim 1 except that it sets forth the claimed

invention as an apparatus rather a method and rejected under the same reasons as

applied above.

Claims 28-29 and 57-58 are rejected under 35 U.S.C. 103(a) as being anticipated by Chung et al. (US 2003/0026462 A1) in view of Stanko (US Patent 20050074126 A1) further in view of Howard et al. (US 2004/0103064 A1) and further in view of Bull et al. (US 6,799,270 B1).

As per claim 28:

The combination of teaching Chung, Stanko, and Howard teach the claimed subject matter.

Chung, Stanko, and Howard are silent about authentication information includes nonce data.

However, Bull teaches authentication request includes nonce data **[Col. 6, lines 44-47; "The nonce Na is a value randomly generated by the client node A 14 that uniquely identifies the authentication request at client node A 14"]**.

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine of Chung, Stanko, and Howard of the invention by including the teaching of Bull because it would have been obvious to use nonce data for each authentication request **[Col. 6, lines 44-47; Bull]**. One of ordinary skill in the art they are used to prevent replay attacks according to the definition of nonce on page 397 of **The Handbook of Applied Cryptography**, by Alfred Menezes et al. Preventing replay attacks prohibits malicious users from gaining access to a secure

system using information gleaned from the eavesdropping of a secure user's

authentication.

As per claim 29:

Chung teaches authentication request includes data comprising identifier data,

signature data, timestamp data, and credential data as described in claim 1 but he does

not teach nonce data.

However, Bull teaches authentication request including nonce data **[Col. 6, lines

44-47].**

Therefore, it would have been obvious to the person of ordinary skill in the art at

the time the invention was made to modify method of Chung of the invention by

including the step of Bull because it would be obvious to use nonce data for each

authentication request **[Col. 6, lines 44-47; Bull].**

Claim 57 is essentially the same as claim 28 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 58 is essentially the same as claim 29 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claims 15-18, 44-47, and 64 are rejected under 35 U.S.C. 103(a) as being anticipated

by **Chung et al.** (US 2003/0026462 A1) in view of **Stanko** (US Patent 20050074126

A1) further in view of **Howard** et al. (US 2004/0103064 A1) and further in view of

Goldstein (US 7,185,206 B2).

As per claim 15:

The combination of teaching Chung, Stanko, and Howard teach the claimed

subject matter.

Stanko further teaches encrypting authentication approval information **[par.**

[0047], lines 6-10; par. [0049]; lines 1-10; par. [0051], lines 5-9; "secure server

204A retrieves the public key corresponding to the private key used to apply the

digital signature to the ticket, uses it to verify the digital signature, and grants

access to client 202 (that is, establishes the session)"].

Chung, Stanko, and Howard are silent about establishing a temporary key and

encrypting said temporary key using said public key to form said corresponding

cryptography information.

However, Goldstein teaches establishing a temporary key and encrypting said

temporary key using said public key to form said corresponding cryptography

information **[Col. 4, lines 35-44; "Most systems use a combination of public-key**

and symmetry. when two computers initiate a secure session, one computer

creates a symmetric key and sends it to the other computer using public-key

encryption. The two computers can then communicate using symmetric-key

encryption. **After the session is finished, each computer discards the symmetric key used for that session. Any additional sessions require that a new symmetric key be created, and the process is repeated"];**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine method of Chung, Stanko, and Howard of the invention by including the step of Goldstein because it would provide to encrypt information to make it secure by preventing unauthorized access along the transmission line **[Goldstein, Col. 3, lines 59-63].**

As per claim 16:

The combination of teaching Chung, Stanko, Howard, and Goldstein teach the claimed subject matter.

Goldstein further teaches the method as recited in claim 15, further comprising:

with said second logic, providing said encrypted temporary key to said first logic; and with said first logic, retrieving said temporary key from said encrypted temporary key using said private key **[Col. 4, lines 35-44; A client includes a first logic and second logic]**.

As per claim 17:

The combination of teaching Chung, Stanko, Howard, and Goldstein teach the claimed subject matter.

Goldstein further teaches the method as recited in claim 16, further comprising:

with said first logic, providing said retrieved temporary key to said second logic;

and with said second logic, retrieving said authentication approval information using

said retrieved temporary key **[Col. 4, lines 35-44; A client includes a first logic and**

second logic].

As per claim 18:

The combination of teaching Chung, Stanko, Howard, and Goldstein teach the

claimed subject matter.

Goldstein further teaches the method as recited in claim 15, wherein said

temporary key includes a symmetric key **[Col. 4, lines 35-36; "most systems use a**

combination of public-key and symmetric"].

Claim 44 is essentially the same as claim 15 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 45 is essentially the same as claim 16 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 46 is essentially the same as claim 17 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 47 is essentially the same as claim 18 except that it sets forth the claimed

invention as computer readable medium rather a method and rejected under the same

reasons as applied above.

Claim 64 is essentially the same as claims 15-17 except that it sets forth the claimed

invention as a system rather a method and rejected under the same reasons as applied

above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Canh Le whose telephone number is 571-270-1380.

The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other

Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

February 4, 2008

Kristine Kincaid
Kristine Kincaid
Supervisory Patent Examiner
AU 2139